



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,505	01/09/2002	Gary J. Cross	AUS920010952US1	6747

35525 7590 11/22/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER

HOFFMAN, BRANDON S

ART UNIT PAPER NUMBER

2136

DATE MAILED: 11/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/042,505	Applicant(s) CROSS, GARY J.	
	Examiner Brandon S. Hoffman	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7,9-17,19-27,29 and 30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7,9-17,19-27,29 and 30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-7, 9-17, 19-27, 29, and 30 are pending in this office action, claims 8, 18, and 28 are newly canceled.
2. Applicant's arguments, filed July 21, 2005, have been considered and are persuasive. However, a new ground of rejection is made.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 21-27, 29, and 30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims recite a computer program product comprising steps implemented on a data processing system using instruction means to cause the data processing system to form a secure radio transmission system. However, the computer program product is not limited to a tangible embodiment. In view of applicant's disclosure, specification page 18, lines 1-19, the instruction means, which are a part of the computer program product, are

provided in a computer readable medium, which is not limited to tangible embodiments, but instead are defined as including both tangible embodiments (e.g., a recordable-type media) and intangible embodiments (e.g., transmission-type media). As such, the claim is not limited to statutory subject matter and is therefore non-statutory.

To overcome this type of 101 rejection the claims need to be amended to include only the physical computer media and not a transmission media or other intangible or non-functional media.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b). Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-7, 9-17, 19-27, 29, and 30 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-30 of copending Application No. 10/042,496. Although the conflicting claims are not identical, they are not patentably distinct from each other because the transmission medium used in each invention does not affect the secured transmission between the first computing device and the second computing device. In both inventions, the first and second computing units perform the encrypting/decrypting operations and the recording/playback of the signal transmitted over the communications medium. The conventional radio and convention cellular devices function as transceivers for the computing devices by passing the encrypted/recorded signal from one point to another.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

8. Claims 1-7, 9-17, 19-27, 29, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baugh et al. (U.S. Patent No. 5,815,553) in view of Herlin et al. (U.S. Patent No. 5,915,021), and further in view of Ashby et al. (U.S. Patent No. 5,305,384).

Regarding claims 1, 11 and 21, Baugh et al. discloses a method/system/computer program product for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:

- Providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, **said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified** (abstract, col. 2, lines 58-62 and fig. 1, ref. num 50, 58, and 62);
- Receiving, within said computer system, an input analog signal from said microphone (col. 2, lines 58-62);
- Encrypting, within said computer system, said input analog signal utilizing public key encryption (col. 8, lines 44-47); and
- Passing said encrypted input analog signal from said computer system to **said microphone port that is included within said unmodified** radio and transmitting said encrypted input analog signal utilizing said **unmodified** radio, wherein radio transmissions from said radio are secured (col. 3, lines 9-14 and fig. 1, ref. num 70 and 74).

Baugh et al. does not specifically teach the input signal is encrypted using public key techniques.

Herlin et al. teaches a method for sending a secure message in a telecommunications system using public key encryption (col. 5, lines 12-35 and col. 9, lines 56-58).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a public key encryption system, as taught by Herlin et al., with the method/system/computer program product of Baugh et al. It would have been obvious for such modifications because the system gains the advantage of securing the recorded message from unauthorized disclosure by an eavesdropper who is monitoring the communication link. By using public key encryption, the recorded message can only be decrypted by the private key that corresponds to the public key used to encrypt the message (see col. 3, lines 60-67 of Herlin et al.).

The combination of Baugh et al. as modified by Herlin et al. do not specifically teach providing a computer system being separate and apart from said radio.

Ashby et al. teaches providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (fig. 1, ref. num 12, separate from the other components).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine connecting a radio output to a computer input, as taught by Ashby et al., with the method/system/computer program product of Baugh et al./Herlin et al. It would have been obvious for such modifications because encrypting communications from a radio, who is directly connected to a computing device, prevents

eavesdropping on police and military communications by encrypting the data directly from the radio (see abstract and col. 1, lines 18-23 of Ashby et al.).

Regarding claims 2,12 and 22, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key (see col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 3,13 and 23, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of encrypting, within said computer system, said input analog signal utilizing said public key (see col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 4,14 and 24, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches comprising the steps of receiving, within a **first** application executing within said computer system, said input analog signal from said microphone; encrypting, utilizing said **first** application, said input analog signal utilizing public key encryption; passing said encrypted input analog signal from said **first** application to said **microphone port of said unmodified** radio (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 5, 15 and 25, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising:

- **Receiving, by said computer system from said microphone, said input analog signal** (see fig. 1, ref. num 50 and 62 of Baugh et al.);
- **Converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format; constantly monitoring, by said first application, inputs received from said microphone; detecting, by said first application, a receipt of said file** (see col. 2, line 63 through col. 3, line 25 of Baugh et al.);
- **In response to a detection by said first application of said receipt of said file, encrypting, by said first application, said file utilizing a public key that is part of a public key/private key key pair assigned to said computer system** (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.); and
- **Passing, by said first application, said encrypted file to said microphone port that is included within said radio and transmitting said encrypted file utilizing said unmodified radio** (see fig. 1, ref. num 12 of Ashby et al.).

Regarding claims 6, 16 and 26, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the steps of:

- Providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, **said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified** (see fig. 1, ref. num 54, 98, and 102 of Baugh et al.);
- Providing a second computer system coupled between **said second** speaker and said second **unmodified** radio, wherein outputs from said second radio are received first by said second computer system before being output to said **second** speaker, said second computer system being separate and apart from said second radio (see fig. 1, ref. num 12, separate from the other components of Ashby et al.);
- Receiving, within said second computer system, an encrypted output from **said second** speaker port included within said **unmodified** second radio (see fig. 1, ref. num 86 of Baugh et al.); and
- Decrypting, within said second computer system, said encrypted output utilizing public key encryption and outputting said decrypted output from said second computer system to said **second** speaker (see col. 8, lines 44-47 of Baugh et al.).

Regarding claims 7, 17 and 27, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising:

- **Constantly monitoring, by a second application that is executing within said second computer system, outputs from said second speaker port** (see col. 3, lines 32-42 of Baugh et al.);
- **Receiving, by said second application, said encrypted output from said second speaker port** (see fig. 1, ref. num 86 of Baugh et al.);
- **Decrypting, by said second application, said encrypted output utilizing public key encryption** (see col. 8, lines 44-47 of Baugh et al.); and
- **Passing, by said second application, said decrypted output from said second application to said second speaker** (see fig. 1, ref. num 98 of Baugh et al.).

Regarding claims 9,19 and 29, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the steps of obtaining, by said second computer system, a private key of said computer system; and decrypting said encrypted **output** utilizing said private key (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 10,20 and 30, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of exchanging said private key between said computer system and said second computer system prior to transmissions of radio signals (see col. 5, lines 31-33 of Herlin et al.).


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon N. H.

BH


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100